1 Virtual Fabrics Switch Support

1.1 Overview

The Virtual Fabric Tagging Header (VFT_Header, see FC-FS-2) allows Fibre Channel frames to be tagged with the Virtual Fabric Identifier (VF_ID) of the Virtual Fabric (VF) to which they belong. Tagged frames (i.e., frames with a VFT_Header) belonging to different Virtual Fabrics may be transmitted over the same physical link (see figure 1). By combining VFT_Headers and other features, Virtual Fabrics provide compartmentalization of access and management. The VFT_Header may be supported by N_Ports, F_Ports and E_Ports.

The use of VFT_Header between E_Ports allows implementation of Virtual Fabrics without requiring any change in the Nx_Port/Fx_Port interface, as shown in figure 1.

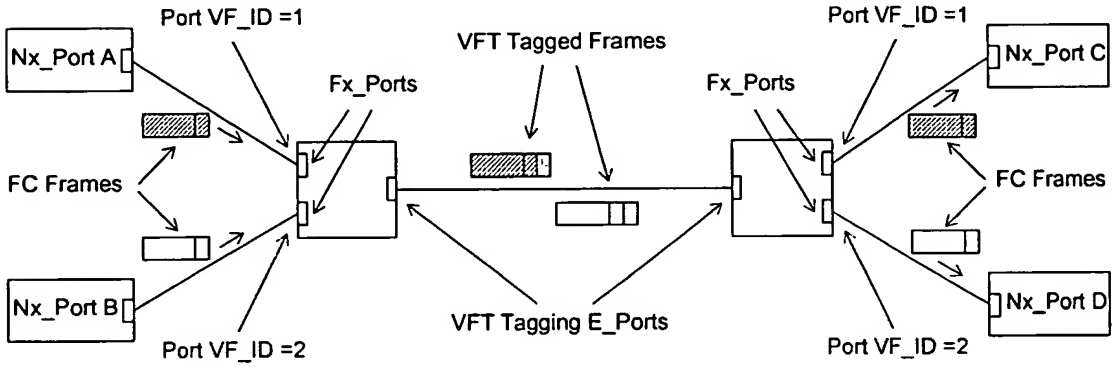


Figure 1 – Virtual Fabrics

Each Fx_Port of a VF capable Switch (i.e., a Switch supporting Virtual Fabrics) shall have a configurable Port VF_ID, so that Nx_Ports may access Virtual Fabric features without modifications. The Port VF_ID shall be associated to any untagged FC frame received by the Fx_Port. A VF capable Switch shall perform frame forwarding by considering the Virtual Fabric the frame belongs to, as identified by the VF_ID. When transmitted between a pair of tagging E_Ports (i.e., E_Ports processing the VFT_Header), each FC frame shall be tagged with a VFT_Header. When a VFT_Header tagged frame is received by a tagging E_Port of a VF capable Switch, the VF_ID carried in the VFT_Header shall be used to perform frame forwarding, together with the D_ID carried in the Frame_Header.

As shown in figure 1, the FC frames sent by Nx_Port A are associated with the Virtual Fabric having VF_ID 1 when received by the Fx_Port. The VF_ID is used by the Switch to perform frame forwarding. Frames transmitted over the tagging E_Port are tagged with a VFT_Header carrying the VF_ID, and their CRC is recomputed (see FC-FS-2). The receiving tagging E_Port retrieves from the VFT tagged frame the VF_ID and uses it together with the D_ID carried in the Frame_Header to route the frames to Nx_Port C. The Fx_Port connected to the destination Nx_Port C removes the VFT_Header, recomputes the CRC (see FC-FS-2) and delivers the original FC frames.

1.2 VF Capable Switch Logical Model

A logical model of a VF capable Switch is shown in figure 2.

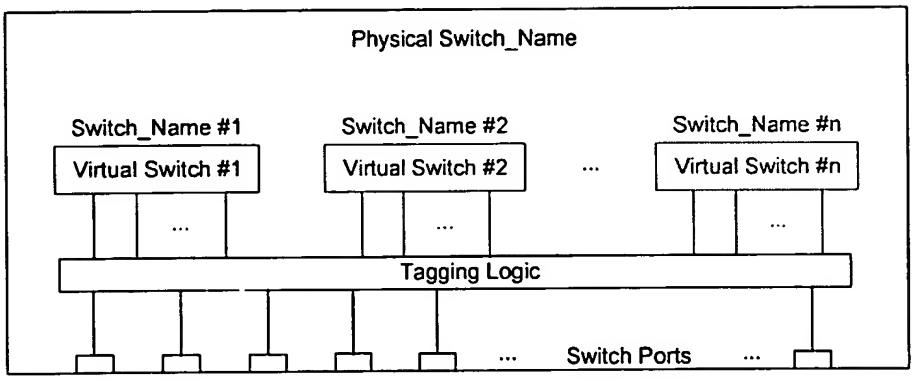


Figure 2 – Logical model of a VF capable Switch

A VF capable Switch is logically a collection of multiple Virtual Switches hosted in the same physical Switch. There is one Virtual Switch per each Virtual Fabric hosted on the physical Switch. A Virtual Switch is logically composed by the components defined in clause 4 of FC-SW-4.

Each Virtual Switch is identified by an unique Switch_Name. In addition, the physical Switch is identified by a unique Physical Switch_Name. Each Virtual Fabric is identified by a 12-bit Virtual Fabric Identifier (VF_ID).

The tagging logic allows to share a physical link across multiple Virtual Fabrics using the VFT_Header. The tagging logic is a multiplexer/demultiplexer driven by the VF_ID in the VFT_Header. Upon receiving a VFT tagged frame from a Switch Port, the tagging logic delivers the frame to the appropriate Virtual Switch (i.e., the Virtual Switch associated with the Virtual Fabric whose VF_ID is carried in the VFT_Header).

When transmitted between a pair of tagging E_Ports, each FC frame shall be tagged with a VFT_Header. A VF capable Switch shall perform frame forwarding by considering the Virtual Fabric the frame belongs to, as identified by the VF_ID.

Each Switch Port of a VF capable Switch shall have a configurable Port VF_ID. The Port VF_ID shall be associated to any untagged FC frame received by the Switch Port. This allows the interconnection of VF capable Switches with non VF capable Switches. Any untagged FC frame received by an E_Port or Fx_Port on a VF capable Switch shall be implicitly associated with the Port VF_ID for processing. The Port VF_ID is then used by the tagging logic to deliver the frame to the appropriate Virtual Switch. In absence of any explicit configuration, the value 001h should be used as default Port VF_ID.

Switches supporting Virtual Fabrics may not receive VFT tagged frames on all Switch Ports. This may occur for the following reasons:

a) A Switch Port is administratively configured to not use VFT_Headers;

b) The port at the far end of a link is administratively configured to not use VFT Headers; or

c) The port at the far end of a link is not capable of processing VFT_Headers.

1.3 Switch_Names Usage

The Switch_Names of the Virtual Switches and the Physical Switch_Name shall be used as follows:

a) In state P5, the Switch_Name of the Virtual Switch associated with the Port VF_ID shall be used when transmitting the ELP SW_ILS;

b) In state P17, the Physical Switch_Name, or the Switch_Name of the Virtual Switch associated with the Port VF_ID, or any other appropriate identity may be used (e.g., when processing the AUTH_ILS SW_ILS, see FC-SP); and

c) When a Switch Port initializes as an E_Port in state P10, the Switch_Name of the Virtual Switch associated with the Port VF_ID shall be used for any subsequent operation or protocol.

1.4 Configuration Information

A VF capable Switch shall maintain the following configuration parameters per each Switch Port:

a) Tagging Administrative Status, used to negotiate the VFT tagging operational mode of the Switch Port (see 1.7.2.2);

b) Port VF_ID (see 1.2 and 1.7.2.3); and

c) Allowed VF_ID List, used to negotiate the list of Virtual Fabrics operational over the Switch Port (see 1.7.2.4).

1.5 Enabling VFT Tagging on Switch Ports

Figure 3 shows the Switch Port Initialization state machine enhanced to enable Virtual Fabrics. In state P13 (i.e., Process ESC) two Switch Ports may negotiate to perform the EVFP processing (see 1.6) if both of them support Virtual Fabrics. The support for Virtual Fabrics is indicated by the ESC Protocol ID value shown in table 1.

Table 1 – ESC Protocol ID for Virtual Fabrics

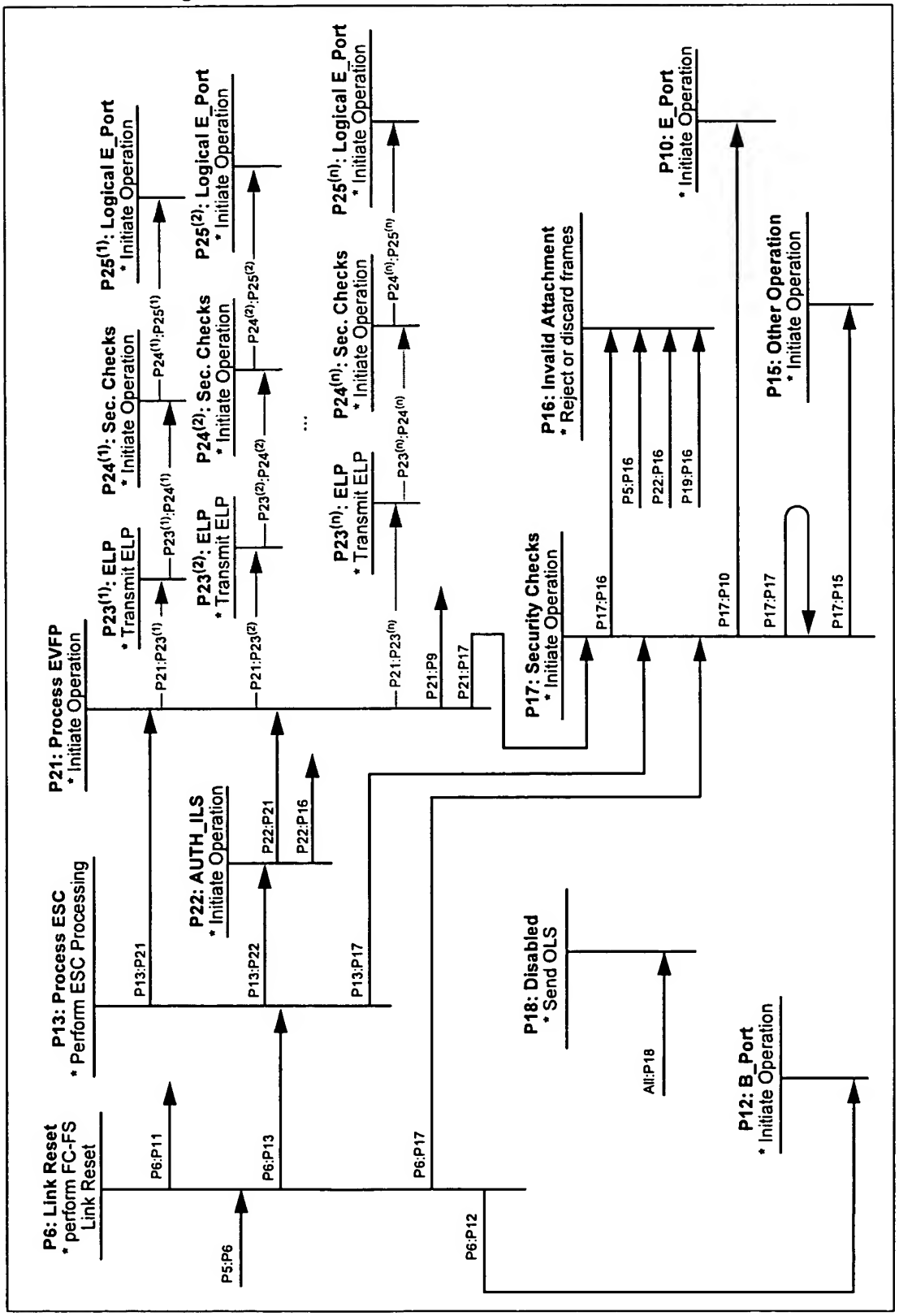
Value	Description
0003h	Virtual Fabrics Supported

The Switch Port sending the ESC request indicates support for Virtual Fabrics by including the Protocol ID shown in table 1 in the ESC payload. The replying Switch Port selects to negotiate Virtual Fabrics parameters by choosing the Protocol ID shown in table 1 in the ESC SW_ACC payload. Then the Switch Port Initialization proceeds to state P21 or to state P22.

If one of the two Switch Ports does not support Virtual Fabrics, the Switch Port Initialization proceeds to state P17 (i.e., Security Checks).

When VFT tagging is enabled on a link, a Link Reset (see FC-FS-2) shall not change the tagging process, while a Link Initialization (see FC-FS-2) shall stop the tagging process and bring the involved Switch Ports to state P0.

Figure 3 – Enhanced Switch Port Initialization State Machine



Transition P13:P21. Occurs when the two Switch Ports negotiated to perform the EVFP processing, and no authentication is required by either Switch Port.

Transition P13:P22. Occurs when the two Switch Ports negotiated to perform the EVFP processing, and authentication is required by at least a Switch Port.

State P22: AUTH_ILS. While in this state an Authentication transaction shall be performed (see FC-SP). The Physical Switch_Name, or the Switch_Name of the Virtual Switch associated with the Port VF_ID, or any other appropriate identity may be used.

Transition P22:P16. Occurs when the Authentication transaction performed in state P22 fails.

Transition P22:P21. Occurs when the Authentication transaction performed in state P22 completes successfully.

State P21: Process EVFP. The Switch Port shall perform EVFP processing as described in 1.6.

Transition P21:P17. Occurs when the EVFP processing determined that VFT tagging is not performed and the two Switch Ports have the same Port VF_ID.

Transition P21:P9. Occurs when the EVFP processing determined that VFT tagging is not performed and the two Switch Ports have a different Port VF_ID.

Transition P21:P23$^{(k)}$. Occurs when the EVFP processing determined that VFT tagging is performed. There is a different state for each Virtual Fabric negotiated to be used on the link. The state for Virtual Fabric K is denoted P23$^{(k)}$.

State P23$^{(k)}$: ELP. In this state the FC frames transmitted by the Switch Port are tagged with the VFT_Header carrying VF_ID K. An ELP, tagged with VF_ID K, is transmitted. This ELP shall carry the Switch Name of the Virtual Switch associated with VF_ID K and the operational parameters (e.g., timeout values, Classes of service) of Virtual Fabric K. No flow control configuration is required in this state, because it is performed in state P5.

Transition P23$^{(k)}$:P24$^{(k)}$. Occurs when the ELP processing in state P23 is completed.

State P24$^{(k)}$: Security Checks. In this state the FC frames transmitted by the Switch Port are tagged with the VFT_Header carrying VF_ID K. The Switch Port initiates and responds to all required security checks (see FC-SP), if any, by using the Switch_Name of the Virtual Switch associated with VF_ID K or any other appropriate identity.

Transition P24$^{(k)}$:P25$^{(k)}$. Occurs when the Security Checks performed in state P24$^{(k)}$ complete successfully.

State P25$^{(k)}$: Logical E_Port. In this state the Switch Port operates as VFT tagging E_Port. FC frames transmitted by the Switch Port are tagged with the VFT_Header carrying VF_ID K. The logical E_Port shall participate in the next phase of Fabric Configuration in Virtual Fabric K. The Switch_Name of the Virtual Switch associated with VF_ID K shall be used for any subsequent operation or protocol in Virtual Fabric K.

1.6 Exchange Virtual Fabrics Parameters Processing

1.6.1 Overview

The Exchange Virtual Fabrics Parameters (EVFP) protocol allows peers of Interconnect_Ports belonging to VF capable Switches to:

a) Negotiate the VFT Tagging operational mode;

b) Verify the consistency of the two Port VF_IDs; and

c) Establish the list of operational Virtual Fabrics across the Inter Switch Link.

An EVFP transaction occurs between an EVFP Initiator and an EVFP Responder. An EVFP transaction (see figure 4) is identified by a unique Transaction Identifier (T_ID), and consists of a synchronizing phase (EVFP_SYNC) followed by a commit phase (EVFP_COMMIT).

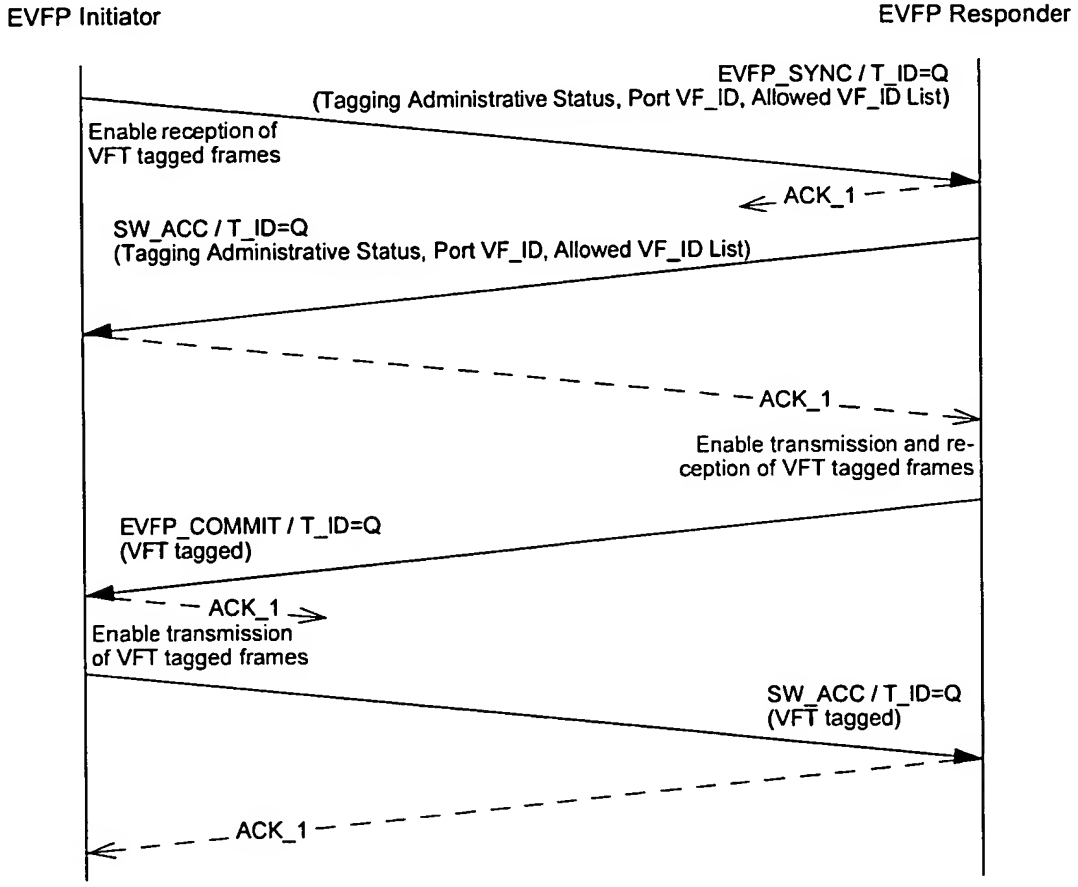


Figure 4 – A Generic EVFP Transaction

The VF_ID value FEFh is used by the EVFP protocol for certain operations and is referred to as Control VF_ID. The EVFP protocol, during the Switch Port Initialization, proceeds as follows:

1) The EVFP Initiator shall start the EVFP transaction by sending the EVFP_SYNC message (see 1.7.2) to the EVFP Responder. In the EVFP_SYNC message, the EVFP Initiator shall specify the Transaction Identifier, and shall send its Physical Switch_Name, together with its Tagging Administrative Status (see 1.7.2.2), Port VF_ID (see 1.7.2.3) and Allowed VF_ID List (see 1.7.2.4). On sending the EVFP_SYNC message the EVFP Initiator enables the reception of VFT tagged frames;

2) The EVFP Responder shall reply with an SW_ACC carrying its Tagging Administrative Status, Port VF_ID and Allowed VF_ID List. Then the EVFP Responder shall determine if VFT Tagging has to be enabled on the link, according to table 11. If VFT Tagging has to be enabled, the EVFP Responder shall go to step 3. If VFT Tagging has not to be enabled, the EVFP Responder shall check the received peer's Port VF_ID:

   A) if the peer's Port VF_ID is not equal to the local Port VF_ID, on completion of the Exchange (i.e., on receiving the ACK_1 for the EVFP_SYNC SW_ACC) the EVFP protocol terminates and the EVFP Responder goes in Isolated state (transition P21:P9, see 1.5); or

   B) if the peer's Port VF_ID is equal to the local Port VF_ID, on completion of the Exchange (i.e., on receiving the ACK_1 for the EVFP_SYNC SW_ACC) the EVFP protocol terminates and the EVFP Responder goes in state P17 (transition P21:P17, see 1.5).

   On receiving the EVFP_SYNC SW_ACC, the EVFP Initiator shall determine if VFT Tagging has to be enabled on the link, according to table 11. If VFT Tagging has to be enabled, on completion of the Exchange (i.e., on sending the ACK_1 for the EVFP_SYNC SW_ACC) the EVFP Initiator shall enable the reception of VFT tagged frames in its Port VF_ID and shall go to step 4. If VFT Tagging has not to be enabled, the EVFP Initiator disables the reception of VFT tagged frames and shall check the received peer's Port VF_ID:

   A) if the peer's Port VF_ID is not equal to the local Port VF_ID, on completion of the Exchange (i.e., on sending the ACK_1 for the EVFP_SYNC SW_ACC) the EVFP protocol terminates and the EVFP Initiator goes in Isolated state (transition P21:P9, see 1.5); or

   B) if the peer's Port VF_ID is equal to the local Port VF_ID, on completion of the Exchange (i.e., on sending the ACK_1 for the EVFP_SYNC SW_ACC) the EVFP protocol terminates and the EVFP Initiator goes in state P17 (transition P21:P17, see 1.5);

3) On completion of the EVFP_SYNC Exchange (i.e., on receiving the ACK_1 for the EVFP_SYNC SW_ACC), the EVFP Responder shall enable both transmission and reception of VFT tagged frames for the Virtual Fabrics operational on the link, computed as explained in 1.7.2.4. Then the EVFP Responder shall send an EVFP_COMMIT message (see 1.7.3), tagged with the peer's Port VF_ID; and

4) On receiving the VFT tagged EVFP_COMMIT, the EVFP Initiator shall enable both transmission and reception of VFT tagged frames for the Virtual Fabrics operational on the link, computed as explained in 1.7.2.4. Then the EVFP Initiator shall send an EVFP_COMMIT SW_ACC message tagged with its Port VF_ID.

When tagging is enabled the EVFP transaction completes successfully on completion of the EVFP_COMMIT Exchange, for both the EVFP Initiator and EVFP Responder. When the EVFP transaction is completed the processing continues independently for each Virtual Fabric operational on the link, as shown by transitions P21:P23$^{(k)}$ (see 1.5).

If two Interconnect_Ports start an EVFP transaction at the same time, or if an Interconnect_Port is acting as an EVFP Initiator and receives an EVFP_SYNC message from the designated EVFP Responder, one of the two EVFP transactions shall be aborted. The Interconnect_Port with the numerically higher Physical Switch_Name shall remain the EVFP Initiator, while the Interconnect_Port with the numerically lower Physical Switch_Name shall become the EVFP Responder. The Interconnect_Port that remains the EVFP Initiator shall reply to the received EVFP_SYNC message with a 'EVFP collision' SW_RJT (see 1.7.1.2). The Interconnect_Port that becomes the EVFP Responder shall reply to the received EVFP_SYNC message and abort its own transaction upon receipt of the SW_RJT.

The EVFP protocol is used also when some Switch Port configuration information (see 1.4) are changed by a management action. The EVFP messages may be carried in FC frames tagged with the Port VF_ID if the EVFP protocol begins while the link is not performing VFT tagging (see 1.6.1). The EVFP messages are carried in FC frames tagged with the Control VF_ID if the EVFP protocol begins while the link is performing VFT tagging (see 1.6.2 and 1.6.3).

1.6.2 Changing the VFT Tagging Mode

When a management action changes the Administrative Tagging Mode of an E_Port belonging to a VF capable Switch that determined during initialization the peer supports the EVFP protocol, the E_Port shall determine if the link has to change its VFT Tagging mode (i.e., if it has to transition from tagging to untagging mode or from untagging to tagging mode) by acting as EVFP Initiator as follows. If the E_Port is currently performing tagging, all EVFP protocol messages shall be tagged with the Control VF_ID. If the E_Port is currently not performing tagging, all EVFP protocol messages shall be untagged.

1) The EVFP Initiator shall start the EVFP transaction by sending the EVFP_SYNC message to the EVFP Responder. The EVFP_SYNC message shall carry the updated Tagging Administrative Status (see 1.7.2.2), Port VF_ID, and the Allowed VF_ID List; and

2) The EVFP Responder shall reply with an SW_ACC carrying its Tagging Administrative Status, Port VF_ID and Allowed VF_ID List. The EVFP Responder shall determine if VFT Tagging has to be changed on the link, according to table 11. The EVFP Responder:

   A) if VFT Tagging has not to be changed, on completion of the Exchange (i.e., on receiving the ACK_1 for the EVFP_SYNC SW_ACC) terminates the EVFP protocol; or

   B) if VFT Tagging has to be changed, on completion of the Exchange (i.e., on receiving the ACK_1 for the EVFP_SYNC SW_ACC) shall perform a link initialization.

   On receiving the EVFP_SYNC SW_ACC, the EVFP Initiator shall determine if VFT Tagging has to be changed on the link, according to table 11. The EVFP Initiator:

   A) if VFT Tagging has not to be changed, on completion of the Exchange (i.e., on sending the ACK_1 for the EVFP_SYNC SW_ACC) terminates the EVFP protocol; or

   B) if VFT Tagging has to be changed, shall participate in the link initialization initiated by the EVFP Responder.

1.6.3 Adding or Removing Virtual Fabrics

When a management action changes the allowed VF_ID Bitmap over a tagging E_Port, the E_Port shall initiate the EVFP protocol by acting as EVFP Initiator as follows. All EVFP protocol messages shall be tagged with the Control VF_ID.

1) The EVFP Initiator shall start the EVFP transaction by sending the EVFP_SYNC message to the EVFP Responder. The EVFP_SYNC message shall carry the Tagging Administrative Status, Port VF_ID, and the updated Allowed VF_ID List (see 1.7.2.4);

2) The EVFP Responder shall reply with an SW_ACC carrying its Tagging Administrative Status, Port VF_ID and Allowed VF_ID List. The EVFP Responder, depending on the resulting operational VF_ID List (see 1.7.2.4):

   A) if the operational VF_ID List did not change, on completion of the Exchange (i.e., on receiving the ACK_1 for the EVFP_SYNC SW_ACC) in the Control VF_ID terminates the EVFP protocol; or

   B) if the operational VF_ID List did change, on completion of the Exchange (i.e., on receiving the ACK_1 for the EVFP_SYNC SW_ACC) in the Control VF_ID goes to step 3.

   On receiving the EVFP_SYNC SW_ACC in the Control VF_ID, the EVFP Initiator, depending on the resulting operational VF_ID List (see 1.7.2.4):

   A) if the operational VF_ID List did not change, on completion of the Exchange (i.e., on sending the ACK_1 for the EVFP_SYNC SW_ACC) in the Control VF_ID terminates the EVFP protocol; or

   B) if the operational VF_ID List did change, on completion of the Exchange (i.e., on sending the ACK_1 for the EVFP_SYNC SW_ACC) in the Control VF_ID goes to step 4.

3) On completion of the EVFP_SYNC Exchange (i.e., on receiving the ACK_1 for the EVFP_SYNC SW_ACC) in the Control VF_ID, the EVFP Responder shall apply the updated operational VF_ID List, enabling the added Virtual Fabrics and disabling the removed Virtual Fabrics. Then the EVFP Responder shall send an EVFP_COMMIT message; and

4) On receiving the EVFP_COMMIT message, the EVFP Initiator shall apply the updated operational VF_ID List, enabling the added Virtual Fabrics and disabling the removed Virtual Fabrics. Then the EVFP Initiator shall send an EVFP_COMMIT SW_ACC message.

When the operational VF_ID List changes, the EVFP transaction completes successfully on completion of the EVFP_COMMIT Exchange for both the EVFP Initiator and EVFP Responder. When the EVFP transaction is completed, the updated operational VF_ID List is operative.

1.6.4 Changing the Port VF_ID

When a management action changes the Port VF_ID of a tagging E_Port, no changes are applied to the link.

When a management action changes the Port VF_ID of a non tagging E_Port, the E_Port shall perform a link initialization.

When a management action changes the Port VF_ID of a Switch Port in Isolated state (i.e., state P9), the Switch Port shall go in state P0.

1.7 Exchange Virtual Fabrics Parameters (EVFP)

1.7.1 EVFP Messages Structure

1.7.1.1 EVFP Request Sequence

Protocol: Exchange Virtual Fabrics Parameters (EVFP) Request Sequence

Format: FT–1

Addressing: The S_ID field shall be set to FFFFFDh, indicating the Fabric Controller of the originating Switch. The D_ID field shall be set to FFFFFDh, indicating the Fabric Controller of the destination Switch.

Payload: Two types of EVFP messages are defined. All EVFP Request messages share the same message structure, shown in table 2.

Table 2 – EVFP Request Payload

Item	Size (Bytes)
EVFP SW_ILS Command Code (TBD)	4
Protocol Version	1
EVFP Message Code	1
Transaction Identifier	2
Physical Switch_Name	8
Reserved	2
Message Payload Length	2
Message Payload	variable

Protocol Version: Shall be set to one.

EVFP Message Code: Specifies the EVFP message that is to be transmitted from the source to the destination. The defined EVFP message codes are shown in table 3.

Table 3 – EVFP Message Codes

Value	Description	Reference
01h	EVFP_SYNC	1.7.2
02h	EVFP_COMMIT	1.7.3
all others	Reserved	

Transaction Identifier: Uniquely identifies an EVFP transaction between two entities. The Transaction Identifier shall be set by the EVFP Initiator, and each subsequent EVFP message shall contain the same value, until the EVFP transaction is completed.

NOTE 1 – The usage of the Transaction Identifier is very similar to the usage of an OX_ID when an Exchange Originator is enforcing uniqueness via the OX_ID mechanism (see FC-FS-2), but it is not related in any way to the OX_ID present in the Fibre Channel frames carrying the EVFP messages.

Physical Switch_Name: Shall be set to the Physical Switch_Name of the originating Switch.

Payload Length: Shall be set to the total length in bytes of the EVFP Payload (i.e., 20 + the Message Payload length).

1.7.1.2 EVFP Reply Sequence

Accept (SW_ACC)
Signifies acceptance of the EVFP request.

Accept Payload: All EVFP Accept messages share the same message structure, shown in table 4.

Table 4 – EVFP Accept Payload

Item	Size (Bytes)
0200 0000h	4
Protocol Version	1
EVFP Message Code	1
Transaction_ID	2
Physical Switch_Name	8
Reserved	2
Message Payload Length	2
Message Payload	variable

The fields in table 4 are the same as defined in table 2.

Service Reject (SW_RJT)
Signifies the rejection of the EVFP request

Table 5 shows the use of Reason Codes and Reason Code Explanations under some error conditions.

Table 5 – SW_RJT Reason Codes

Error Condition	Reason Code	Reason Code Explanation
EVFP SW_ILS not supported	Command Not Supported	No Additional Explanation
EVFP collision	Unable to perform command request	Command Already in Progress
EVFP Protocol Version not supported	Invalid Revision Level	No Additional Explanation
EVFP_COMMIT before EVFP_SYNC	Logical Error	No Additional Explanation
Insufficient Resources	Unable to Perform Command Request	Insufficient Resources Available
Invalid Payload Message	Protocol Error	No Additional Explanation

1.7.2 EVFP_SYNC Message

1.7.2.1 Overview

The EVFP_SYNC Message Payload carries a list of descriptors. Each descriptor is self-identifying (see table 7). The format of the EVFP_SYNC Message Payload is shown in table 6. This Message Payload is used in both EVFP_SYNC Request and EVFP_SYNC Accept.

Table 6 – EVFP_SYNC Message Payload

Item	Size (Bytes)	Reference
Descriptor #1 = Tagging Administrative Status	8	1.7.2.2
Descriptor #2 = Port VF_ID	8	1.7.2.3
Descriptor #3 = Allowed VF_ID List	516	1.7.2.4
...		
Descriptor #m	variable	

All descriptors share the same format, shown in table 7.

Table 7 – Descriptor Format

Item	Size (Bytes)
Descriptor Control	1
Descriptor Type	1
Descriptor Length	2
Descriptor Value	variable

Descriptor Control: Specifies the behavior of the receiving entity if the descriptor is unsupported. The defined codes are shown in table 8.

Table 8 – Descriptor Control Codes

Value	Description
01h	Critical. Abort the EVFP transaction if the descriptor is unsupported.[a]
02h	Non critical. Skip the descriptor if unsupported and continue the EVFP transaction.[a]
all others	Reserved

[a] The Descriptor Control provides extensibility to the protocol. An implementation supporting a subset of the descriptors is able to process the unknown ones as specified by the Descriptor Control value.

Descriptor Type: Specifies the type of the descriptor.

Descriptor Length: Specifies the length in bytes of the Descriptor Value.

1.7.2.2 Tagging Administrative Status Descriptor

The format of the Tagging Administrative Status descriptor is shown in table 9.

Table 9 – Tagging Administrative Status Descriptor

Item	Size (Bytes)
Descriptor Control = 01h	1
Descriptor Type = 01h	1
Descriptor Length = 0004h	2
Administrative Tagging Mode	4

The defined Administrative Tagging Modes are shown in table 10.

Table 10 – Administrative Tagging Modes

Value	Notation	Description
0000 0001h	OFF	The Interconnect_Port shall not perform VFT Tagging
0000 0002h	ON	The Interconnect_Port may perform VFT Tagging if the peer does not prohibit it
0000 0003h	AUTO	The Interconnect_Port may perform VFT Tagging if the peer request it

In absence of any explicit configuration, the default Administrative Tagging Mode of a Switch Port of a VF capable Switch should be AUTO.

Table 11 shows how VFT tagging is negotiated between peer Interconnect_Ports.

Table 11 – Tagging Mode Negotiation

		Peer Tagging Mode		
		OFF	ON	AUTO
Local Tagging Mode	OFF	Non Tagging	Non Tagging	Non Tagging
	ON	Non Tagging	Tagging	Tagging
	AUTO	Non Tagging	Tagging	Non Tagging

1.7.2.3 Port VF_ID Descriptor

The format of the Port VF_ID descriptor is shown in table 12.

Table 12 – Port VF_ID Descriptor

Item	Size (Bytes)
Descriptor Control = 01h	1
Descriptor Type = 02h	1
Descriptor Length = 0004h	2
Port Flags	2
Port VF_ID	2

Port Flags: Reserved. Shall be set to zero.

Port VF_ID: The 12 least significant bit of this field shall be set to the Port VF_ID. The four most significant bit shall be set to zero. In absence of any explicit configuration, the value 001h should be used as Port VF_ID.

1.7.2.4 Allowed VF_ID List Descriptor

The format of the Allowed VF_ID List descriptor is shown in table 13.

Table 13 – Allowed VF_ID List Descriptor

Item	Size (Bytes)
Descriptor Control = 01h	1
Descriptor Type = 03h	1
Descriptor Length = 0200h	2
VF_ID Bitmap	512

VF_ID Bitmap: Each Virtual Fabric is identified by a bit in the VF_ID Bitmap. The high-order bit represents VF_ID zero, each successive bit represents the successive VF_ID, and the low-order bit represents VF_ID 4095. Virtual Fabric K is allowed on the Interconnect_Port if the Kth bit of the VF_ID Bitmap is set to one; is disallowed if the Kth bit of the VF_ID Bitmap is set to zero.

The list of Virtual Fabrics operational over a link is computed by performing a bit-wise 'AND' between the received VF_ID Bitmap and the locally configured VF_ID Bitmap.

1.7.3 EVFP_COMMIT Message

Both EVFP_COMMIT Request and EVFP_COMMIT Accept have a NULL Message Payload.